GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

November 22, 2004

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Subject: GAO Review of Financial Market Organizations' Information Security

Dear Mr. Dingell:

This letter confirms our commitment to study the adequacy of the information security practices at selected financial market organizations based on your letter to the Comptroller General. This work is a continuation of an effort that we began as part of your committee's request that GAO follow up on its previous reports on the preparedness of financial market organizations to prevent disruptions and recover from terrorist attacks. On September 27, 2004, we issued a report to you that summarizes the results of our work we have completed to respond to most of your request.[1] This study is to complete the more in-depth work we have been conducting looking at the information security of some of the key financial market organizations discussed in that report. Based on the design that we have discussed with your staff, we will complete our work and issue a report to you by April 15, 2005. Please see enclosure I for the list of requesters with whom we will be coordinating. Enclosure II sets forth the key aspects of the study.

We look forward to working with you and your staff on this assignment. Should you have any questions, please contact me on (202) 512-9073 or hillmanr@gao.gov or, Cody Goebel, Assistant Director, on (202) 512-7329 or goebelc@gaogov.

Sincerely yours,

Richard J. Hillman
Director, Financial Markets
and Community Investment

Enclosures - 2

cc: Consuela Washington
Pete Filon

[1]See GAO, *Potential Terrorist Attacks: Additional Actions Needed to Better Prepare Critical Financial Market Participants*, GAO-04-984 (Washington, D.C.: Sept. 27, 2004).

ENCLOSURE I

LIST OF REQUESTERS

The Honorable Joe Barton
Chairman
Committee on Energy and Commerce
House of Representatives

The Honorable Fred Upton
Chairman
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable Edward J. Markey
Ranking Minority Member
Subcommittee on Telecommunications and the Internet
Committee on Energy and Commerce
House of Representatives

The Honorable Cliff Stearns
Chairman
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
House of Representatives

The Honorable Jan Schakowsky
Ranking Minority Member
Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
House of Representatives

Enclosure

Terms of the Work

Objectives/Key Questions

To review the adequacy of the information security programs of selected financial market organizations, we are assessing whether these organizations information security programs have

(1) appropriate policies and management oversight,

(2) controls that appear to be sufficient to prevent unauthorized access,

(3) intrusion detection systems that appear capable of identifying cyber attacks on all critical systems, and

(4) regular vulnerability assessments that reviewed all relevant aspects of all critical systems.

Scope

The organizations that we are reviewing include seven critical financial market organizations. These organizations were selected on the basis that, because they either perform a unique function necessary to the markets or operate on large such a scale, a disruption in the operations of one of these organizations would severely impair the ability of the financial markets to function.

Methodology

Conducting site visits at each of the organizations, we are assessing the adequacy of their information security programs by

(1) using professional judgment and government information security standards to assess appropriateness of security policies and management oversight,

(2) using professional knowledge of attack techniques and control effectiveness to assess the whether existing controls appear to be sufficient to prevent unauthorized access,

(3) obtaining descriptions and inspecting where possible existing intrusion detection systems to assess whether they appear capable of identifying cyber attacks on all critical systems, and

(4) reviewing assessment reports and testing results done at these organizations to identify whether regular assessments of the vulnerabilities of all relevant aspects of these organizations' critical systems have been reviewed regularly.

The work will be done in accordance with Generally Accepted Government Auditing Standards (GAGAS).

Product Type

Because of the highly sensitive nature of the operations we are reviewing at these organizations and their importance to the overall markets, the results of this work will be summarized and reported in a correspondence. This correspondence will include high-level descriptions of the work performed and the actions being taken by the organizations in response to any areas for improvement our work identifies. We will obtain comments from the Securities and Exchange Commission and the Board of Governors of the Federal Reserve System on a written draft of this product prior to issuance.

Product Delivery Date(s)

This product will be issued by April 15, 2005.

Reporting on Job Status

We will provide periodic updates on the progress of work and the development of the product throughout and when desired by the requestors' staff.